



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide



[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Authentication in distributed systems: theory and practice

Full text Pdf (2.33 MB)

Source **ACM Symposium on Operating Systems Principles** [archive](#)
Proceedings of the thirteenth ACM symposium on Operating systems principles [table of contents](#)
Pacific Grove, California, United States
Pages: 165 - 182
Year of Publication: 1991
ISSN:0163-5980
[Also published in ...](#)

Authors [Butler Lampson](#) Systems Research Center, Digital Equipment Corporation, 130 Lytton Ave., Palo Alto, CA
[Martin Abadi](#) Systems Research Center, Digital Equipment Corporation, 130 Lytton Ave., Palo Alto, CA
[Michael Burrows](#) Systems Research Center, Digital Equipment Corporation, 130 Lytton Ave., Palo Alto, CA
[Edward Wobber](#) Systems Research Center, Digital Equipment Corporation, 130 Lytton Ave., Palo Alto, CA

Sponsor [SIGOPS](#): ACM Special Interest Group on Operating Systems

Publisher ACM Press New York, NY, USA

Additional Information: [abstract](#) [references](#) [cited by](#) [index terms](#) [collaborative colleagues](#) [peer to peer](#)

Tools and Actions: [Find similar Articles](#) [Review this Article](#)
[Save this Article to a Binder](#) Display Formats: [BibTex](#) [EndNote](#) [ACM Ref](#)

DOI Bookmark: Use this link to bookmark this Article: <http://doi.acm.org/10.1145/121132.121160>
[What is a DOI?](#)

ABSTRACT






We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegation of authority. The theory explains how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We use the theory to explain many existing and proposed mechanisms for security. In particular, we describe the system we have built. It passes principals efficiently as arguments or results of remote procedure calls, and it handles public and shared key encryption, name lookup in a large name space, groups of principals, loading programs, delegation, access control, and revocation.





REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.







- 1 M. Abadi, M. Burrows, C. Kaufman, and B. Lampson. Authentication and delegation with smart-cards. To appear in Theoretical Aspects of Computer Software, Springer, 1991. Also

research report 67, Systems Research Center, Digital Equipment Corp., Palo Alto, Oct. 1990.

- 2 Martín Abadi , Michael Burrows , Butler W. Lampson , Gordon D. Plotkin, A Calculus for Access Control in Distributed Systems, Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, p.1-23, August 11-15, 1991
- 3 A. Birrell, B. Lampson. R. Needham, and M. Schroeder. Global authentication without global trust. Proc. IEEE Symposium on Security and Privacy, Oakland, 1986, 223-230.
-  4 Michael Burrows , Martin Abadi , Roger Needham, A logic of authentication, ACM Transactions on Computer Systems (TOCS), v.8 n.1, p.18-36, Feb. 1990
- 5 CCITT. Information processing systems -- Open systems interconnection --The directory authentication framework. CCITT 1988 Recommendation X 509. Also ISO/IEC 9594-8:1989.
- 6 P. G. Comba, Exponentiation cryptosystems on the IBM PC, IBM Systems Journal, v.29 n.4, p.526-538, 1990
-  7 Don Davis , Ralph Swick, Network security via private-key certificates, ACM SIGOPS Operating Systems Review, v.24 n.4, p.64-67, Oct. 1990
-  8 Dorothy E. Denning, A lattice model of secure information flow, Communications of the ACM, v.19 n.5, p.236-243, May 1976
- 9 Department of Defense. Trusted Computer System Evaluation Criteria. DOD 5200.28-STD, 1985.
- 10 W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Information Theory IT-22, 6, Nov. 1976, 644-654.
- 11 H. Eberle, Systems Research Center, Digital Equipment Corp., Palo Alto. Private communication.
- 12 M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson. The Digital distributed system security architecture. Proc. 12th National Computer Security Conference, NIST/NCSC, Baltimore, 1989, 305- 319.
- 13 M. Gasser and E. McDermott. An architecture for practical delegation in a distributed system. Proc. IEEE Symposium on Security and Privacy, Oakland, 1990, 20-30.
- 14 B. Herbison. Low cost outboard cryptographic support for SILS and SP4. Proc. 13th National Computer Security Conference, NIST/NCSC, Baltimore, 1990, 286-295.
- 15 J. Kohl, C. Neuman, and J. Steiner. The Kerberos network authentication service. Version 5, draft 3, Project Athena, MIT, Oct. 1990.
-  16 Butler W. Lampson, Protection, ACM SIGOPS Operating Systems Review, v.8 n.1, p.18-24, January 1974
- 17 J. Linn. Practical authentication for distributed systems. Proc. IEEE Symposium on Security and Privacy, Oakland, 1990, 31-40.
- 18 National Bureau of Standards. Data Encryption Standard. FIPS Pub. 46, Jan. 1977.
-  19 Roger M. Needham , Michael D. Schroeder, Using encryption for authentication in large networks of computers, Communications of the ACM, v.21 n.12, p.993-999, Dec. 1978
- 20 C. Neuman. Proxy-based authorization and accounting for distributed systems. Technical report 91-02-01, University of Washington, Seattle, March 1991.

-  21 R. L. Rivest , A. Shamir , L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, v.21 n.2, p.120-126, Feb. 1978
- 22 R. Rivest. The MD4 message digest algorithm TM 434, Laboratory for Computer Science, MIT, Oct. 1990.
-  23 J. H. Saltzer , D. P. Reed , D. D. Clark, End-to-end arguments in system design, ACM Transactions on Computer Systems (TOCS), v.2 n.4, p.277-288, Nov. 1984
-  24 M. Shand , P. Bertin , J. Vuillemin, Hardware speedups in long integer multiplication, Proceedings of the second annual ACM symposium on Parallel algorithms and architectures, p.138-145, July 02-06, 1990, Island of Crete, Greece
- 25 J. Steiner, C. Neuman, and J Schiller. Kerberos: An authentication service for open network systems. Proc. Usenix Winter Conference, Usenix Association, Berkeley, CA, Feb. 1988, 19t-202.
- 26 J. Tardo and K. Alagappan. SPX. Global authentication using public key certificates. Proc. 4th National Computer Security Conference, NIST/NCSC, Baltimore, 1991.
-  27 Victor L. Voydock , Stephen T. Kent, Security Mechanisms in High-Level Network Protocols, ACM Computing Surveys (CSUR), v.15 n.2, p.135-171, June 1983

CITED BY 11

-  Thomas Y. C. Woo , Simon S. Lam, A framework for distributed authorization, Proceedings of the 1st ACM conference on Computer and communications security, p.112-118, November 03-05, 1993, Fairfax, Virginia, United States
- Charles Rackoff, Some definitions, protocols and proofs about secure authentication, Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research, November 09-12, 1992, Toronto, Ontario, Canada
- Gerald A. Winters , Toby J. Teorey, Managing heterogeneous distributed computing systems: using information repositories, Proceedings of the 1993 conference of the Centre for Advanced Studies on Collaborative research: distributed computing, October 24-28, 1993, Toronto, Ontario, Canada
- Woei-Jiunn Tsaor , Shi-Jinn Horng, Auditing Causal Relationships of Group Multicast Communications in Group-Oriented Distributed Systems, The Journal of Supercomputing, v.18 n.1, p.25-45, Jan. 2001
-  Andrew C. Myers , Barbara Liskov, A decentralized model for information flow control, ACM SIGOPS Operating Systems Review, v.31 n.5, p.129-142, Dec. 1997
-  Edward D. Lazowska, Recent trends in experimental operating systems research, Proceedings of the twelfth annual ACM symposium on Principles of distributed computing, p.13-19, August 15-18, 1993, Ithaca, New York, United States
-  Timothy Mann , Andrew Birrell , Andy Hisgen , Charles Jerian , Garret Swart, A coherent distributed file cache with directory write-behind, ACM Transactions on Computer Systems (TOCS), v.12 n.2, p.123-164, May 1994
-  Andrew C. Myers , Barbara Liskov, Protecting privacy using the decentralized label model, ACM Transactions on Software Engineering and Methodology (TOSEM), v.9 n.4, p.410-442, Oct. 2000
-  Yun Fu , Jeffrey Chase , Brent Chun , Stephen Schwab , Amin Vahdat, SHARP: an architecture for secure resource peering, Proceedings of the nineteenth ACM symposium on Operating systems principles, October 19-22, 2003, Bolton Landing, NY, USA



H. M. Gladney, Access control for large collections, ACM Transactions on Information Systems (TOIS), v.15 n.2, p.154-194, April 1997

Franck Cappello , Samir Djilali , Gilles Fedak , Thomas Herault , Frédéric Magniette , Vincent Néri , Oleg Lodygensky, Computing on large-scale distributed systems: Xtrem Web architecture, programming models, security, tests and convergence with grid, Future Generation Computer Systems, v.21 n.3, p.417-437, 1 March 2005

INDEX TERMS

Primary Classification:

D. Software



D.4 OPERATING SYSTEMS



D.4.6 Security and Protection



Subjects: Authentication

Additional Classification:

D. Software



D.4 OPERATING SYSTEMS



D.4.6 Security and Protection



Subjects: Cryptographic controls; Access controls



D.4.7 Organization and Design



Subjects: Distributed systems

General Terms:

Algorithms, Security, Theory

Collaborative Colleagues:

Martín Abadi:	Eric Allender	Cédric Fournet	Leslie Lamport	Gordon D. Plotkin
	Bowen Alpern	Nissim Francez	Butler Lampson	Jon G. Riecke
	Krzysztof R. Apt	Neal Glew	Butler W. Lampson	Phillip Rogaway
	Anindya	Georges Gonthier	Leonid Libkin	Andrei Sabelfeld
	Banerjee	Andrew D. Gordon	Zohar Manna	Fred B. Schneider
	Roberto Bellucci	Joseph Y. Halpern	Florian Matthes	Raymie Stata
	Andrew Birrell	Nevin Heintze	Stephan Merz	Mark R. Tuttle
	Bruno Blanchet	Lane A. Hemachandra	Greg Morrisett	Ramesh
	Andrei Z. Broder	Jan Jürjens	Roger Needham	Viswanathan
	Michael Burrows	Shmuel Katz	Roger M. Needham	Bogdan Warinschi
	Mike Burrows	C. Kaufman	Frank Pfenning	Edward Wobber
	Luca Cardelli	Jean-Jacques Lévy	Benjamin Pierce	Pierre Wolper
	Pierre-Louis	John Lamping	Gordon Plotkin	Leendert van
	Curien			Doorn
	Joan			
	Feigenbaum			
Michael	Martín Abadi	Roger Needham	Edward Wobber	
Burrows:	Martin Abadi	Roger M. Needham		
	Thomas	Greg Nelson		
	Anderson	Gordon Plotkin		
	Matthias	Gordon D. Plotkin		
	Hausner	Stefan Savage		
	Charles Jerian	Daniel J. Scalesk		

	C. Kaufman	Michael D. Schroeder		
	Butler Lampson	Patrick Sobalvarro		
	Butler W. Lampson	Chandramohan A. Thekkath		
	K. Rustan M. Leino			
	Timothy Mann			
Butler Lampson:	Martín Abadi	Paul England	John Manferdelli	Terry Winograd
	Victor R. Basili	Stu Feldman	Timothy Mann	Edward Wobber
	Laszlo Belady	Stuart I. Feldman	Marcus Peinado	
	Barry Boehm	Cordell Green	Gordon Plotkin	
	Frederick Brooks	Charles Jerian	Lawrence A. Rowe	
	James Browne	Jean-Jacques Lévy	Venkatachary	
	Michael Burrows	Duncan Lawrie	Srinivasan	
	Roberto De Prisco	Nancy Leveson	George Varghese	
	Richard DeMillo	Barbara Liskov	Mark Weiser	
	Peter Deutsch	Nancy Lynch	Bryan Willman	
			Jeannette Wing	
Edward Wobber:	Martín Abadi			
	Andrew Birrell			
	Michael Burrows			
	Mike Burrows			
	Butler Lampson			
	Greg Nelson			
	Susan Owicki			
	Raymie Stata			
	Leendert van Doorn			

✎ **Peer to Peer - Readers of this Article have also read:**

- [Data structures for quadtree approximation and compression](#) **Communications of the ACM** 28, 9
Hanan Samet
- [A hierarchical single-key-lock access control using the Chinese remainder theorem](#) **Proceedings of the 1992 ACM/SIGAPP Symposium on Applied computing**
Kim S. Lee , Huizhu Lu , D. D. Fisher
- [The GemStone object database management system](#) **Communications of the ACM** 34, 10
Paul Butterworth , Allen Otis , Jacob Stein
- [An intelligent component database for behavioral synthesis](#) **Proceedings of the 27th ACM/IEEE conference on Design automation**
Gwó-Dong Chen , Daniel D. Gajski
- [Putting innovation to work: adoption strategies for multimedia communication systems](#) **Communications of the ACM** 34, 12
Ellen Francik , Susan Ehrlich Rudman , Donna Cooper , Stephen Levine

✎ **This Article has also been published in:**

- [ACM SIGOPS Operating Systems Review](#)
Volume 25 , Issue 5 Oct. 1991

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)